EchoLogg

Vertrag zur Auftragsverarbeitung (AVV) nach Art. 28 DSGVO

Anlage und zwingender Bestandteil des EchoLogg-Endnutzer-Lizenzvertrags (EULA)

Zwischen dem Lizenznehmer der Software EchoLogg (nachfolgend **„Verantwortlicher“**) und der mit.data GmbH, Kuhlmannstr. 10, 48282 Emsdetten (nachfolgend **„Auftragsverarbeiter“**).

Stand: 01.07.2026 · Version: 1.0

Präambel

Dieser Vertrag konkretisiert die datenschutzrechtlichen Pflichten der Parteien aus dem EULA. Er gilt für alle Verarbeitungen personenbezogener Daten, die der Auftragsverarbeiter im Auftrag des Verantwortlichen vornimmt, insbesondere bei Nutzung des optionalen Cloud-Modus (serverseitige Spracherkennung) sowie bei Support- oder Fernwartungsleistungen mit Zugriff auf personenbezogene Daten. Er ist zwingender, integraler Bestandteil des EULA und wird mit dessen Annahme wirksam; einer gesonderten Unterzeichnung bedarf es nicht. Auf Wunsch stellen die Parteien eine unterzeichnete Fassung in Textform wechselseitig zur Verfügung.

§ 1 Gegenstand und Dauer

(1) Gegenstand des Auftrags ergibt sich aus dem EULA und der Leistungsbeschreibung der Software; Einzelheiten der Verarbeitung sind in Anlage 1 festgelegt.

(2) Die Dauer dieses Vertrags entspricht der Laufzeit des EULA. Eine isolierte Kündigung dieses Vertrags ist ausgeschlossen; das Recht zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt.

§ 2 Art, Zweck und Ort der Verarbeitung, Datenarten, Betroffene

(1) Art und Zweck der Verarbeitung, die Arten personenbezogener Daten und die Kategorien betroffener Personen ergeben sich aus Anlage 1. Die Verarbeitung kann besondere Kategorien personenbezogener Daten im Sinne des Art. 9 DSGVO umfassen (z. B. Gesundheitsdaten in medizinischen Diktaten).

(2) Die Verarbeitung findet ausschließlich in der Bundesrepublik Deutschland, in einem Mitgliedstaat der Europäischen Union oder in einem Vertragsstaat des EWR statt. Eine Verarbeitung in Drittländern erfolgt nur auf dokumentierte Weisung des Verantwortlichen und nur, wenn die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

§ 3 Verantwortlichkeit und Weisungsrecht

(1) Der Verantwortliche ist im Rahmen dieses Vertrags für die Einhaltung der datenschutzrechtlichen Vorschriften verantwortlich, insbesondere für die Rechtmäßigkeit der Datenverarbeitung und die Wahrung der Betroffenenrechte.

(2) Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet ist; in einem solchen Fall teilt er dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht verbietet. Die Nutzung der Software einschließlich ihrer Konfiguration durch den Verantwortlichen gilt als Weisung im Sinne dieses Vertrags.

(3) Weisungen bedürfen der Textform. Mündliche Weisungen sind unverzüglich in Textform zu bestätigen. Weisungsberechtigte und -empfänger können die Parteien in Textform benennen.

(4) Ist der Auftragsverarbeiter der Auffassung, dass eine Weisung gegen die DSGVO oder andere Datenschutzbestimmungen verstößt, informiert er den Verantwortlichen unverzüglich; er ist berechtigt, die Durchführung bis zur Bestätigung oder Änderung der Weisung auszusetzen.

§ 4 Pflichten des Auftragsverarbeiters

(1) Vertraulichkeit: Der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Soweit der Verantwortliche einer Berufsverschwiegenheit unterliegt (insbesondere § 203 StGB), verpflichtet der Auftragsverarbeiter die mitwirkenden Personen entsprechend § 203 Abs. 4 StGB zur Geheimhaltung und weist dies auf Verlangen nach.

(2) Technische und organisatorische Maßnahmen: Der Auftragsverarbeiter trifft die in Anlage 2 beschriebenen Maßnahmen nach Art. 32 DSGVO und entwickelt sie dem Stand der Technik entsprechend fort. Anpassungen sind zulässig, sofern das vereinbarte Schutzniveau nicht unterschritten wird; wesentliche Änderungen werden dokumentiert.

(3) Unterstützung: Der Auftragsverarbeiter unterstützt den Verantwortlichen mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung der Betroffenenrechte (Art. 12–23 DSGVO) sowie bei den Pflichten aus Art. 32 bis 36 DSGVO (Sicherheit der Verarbeitung, Meldung von Verletzungen, Datenschutz-Folgenabschätzung, vorherige Konsultation) unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen.

(4) Der Auftragsverarbeiter führt ein Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DSGVO und benennt dem Verantwortlichen auf Anfrage einen Ansprechpartner für Datenschutzfragen sowie – soweit benannt – seinen Datenschutzbeauftragten.

(5) Anfragen betroffener Personen, die den Auftragsverarbeiter unmittelbar erreichen, leitet er unverzüglich an den Verantwortlichen weiter und beantwortet sie nicht selbst, sofern keine anderslautende Weisung vorliegt.

(6) Kontrollen der Aufsichtsbehörde, die die Auftragsverarbeitung betreffen, zeigt der Auftragsverarbeiter dem Verantwortlichen unverzüglich an, soweit rechtlich zulässig.

§ 5 Unterauftragsverarbeiter

(1) Der Verantwortliche erteilt hiermit die allgemeine Genehmigung zur Einschaltung von Unterauftragsverarbeitern (Art. 28 Abs. 2 Satz 1 DSGVO). Die zum Vertragsschluss eingesetzten Unterauftragsverarbeiter sind in Anlage 3 aufgeführt; die jeweils aktuelle Liste ist unter www.echologg.com/avv abrufbar.

(2) Der Auftragsverarbeiter informiert den Verantwortlichen über jede beabsichtigte Hinzuziehung oder Ersetzung eines Unterauftragsverarbeiters mindestens vier Wochen vor deren Wirksamwerden in Textform (E-Mail an die vom Verantwortlichen hinterlegte Lizenz-E-Mail-Adresse genügt) und aktualisiert die Liste nach Absatz 1.

(3) Der Verantwortliche kann der Änderung innerhalb von vier Wochen nach Zugang der Information aus wichtigem datenschutzrechtlichem Grund in Textform widersprechen. Im Fall des Widerspruchs wird der Auftragsverarbeiter die Verarbeitung wahlweise ohne den betreffenden Unterauftragsverarbeiter fortsetzen oder eine sonstige zumutbare Abhilfe anbieten. Ist beides nicht möglich oder unzumutbar, sind beide Parteien berechtigt, den von der Änderung betroffenen Leistungsteil (insbesondere den Cloud-Modus) mit einer Frist von zwei Wochen in Textform zu kündigen; bereits entrichtete Entgelte für nicht erbrachte Leistungszeiträume dieses Leistungsteils werden anteilig erstattet. Widerspricht der Verantwortliche nicht fristgerecht, gilt die Änderung als genehmigt.

(4) Der Auftragsverarbeiter schließt mit jedem Unterauftragsverarbeiter einen Vertrag, der diesem im Wesentlichen dieselben Datenschutzpflichten auferlegt, wie sie in diesem Vertrag festgelegt sind (Art. 28 Abs. 4 DSGVO). Kommt der Unterauftragsverarbeiter seinen Pflichten nicht nach, haftet der Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten des Unterauftragsverarbeiters.

(5) Keine Unterauftragsverhältnisse im Sinne dieser Regelung sind Nebenleistungen ohne inhaltlichen Datenzugriff, etwa Telekommunikations-, Post- und Transportleistungen, Reinigungs- und Bewachungsdienste sowie Wartung, sofern ein Zugriff auf personenbezogene Daten ausgeschlossen ist; der Auftragsverarbeiter stellt dies durch angemessene Vereinbarungen und Maßnahmen sicher.

§ 6 Meldung von Verletzungen des Schutzes personenbezogener Daten

(1) Der Auftragsverarbeiter meldet dem Verantwortlichen jede Verletzung des Schutzes personenbezogener Daten, die die Auftragsverarbeitung betrifft, unverzüglich nach Bekanntwerden.

(2) Die Meldung enthält – soweit verfügbar – mindestens die Angaben nach Art. 33 Abs. 3 DSGVO. Der Auftragsverarbeiter unterstützt den Verantwortlichen bei dessen Melde- und Benachrichtigungspflichten nach Art. 33 und 34 DSGVO und ergreift unverzüglich angemessene Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen.

§ 7 Nachweise und Kontrollrechte

(1) Der Auftragsverarbeiter stellt dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten zur Verfügung. Der Nachweis kann insbesondere durch aktuelle Testate, Zertifizierungen oder geeignete Selbstauskünfte (z. B. TOM-Dokumentation, an ISO/IEC 27001 orientierte ISMS-Nachweise) erbracht werden.

(2) Der Verantwortliche ist berechtigt, Überprüfungen – einschließlich Inspektionen vor Ort – selbst oder durch einen zur Verschwiegenheit verpflichteten, nicht im Wettbewerb zum Auftragsverarbeiter stehenden Prüfer durchzuführen. Kontrollen erfolgen nach vorheriger Ankündigung mit angemessener Frist (in der Regel zwei Wochen), während der üblichen Geschäftszeiten, ohne unverhältnismäßige Störung des Betriebs und höchstens einmal jährlich, es sei denn, ein konkreter Anlass erfordert weitergehende Kontrollen. Betriebs- und Geschäftsgeheimnisse des Auftragsverarbeiters sowie Daten Dritter sind zu wahren.

§ 8 Löschung und Rückgabe

(1) Sprachdaten im Cloud-Modus werden ausschließlich zur unmittelbaren Transkription verarbeitet und nicht über den Verarbeitungsvorgang hinaus gespeichert (Anlage 1). Kopien oder Duplikate werden ohne Wissen des Verantwortlichen nicht erstellt; hiervon ausgenommen sind technisch erforderliche Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind.

(2) Nach Abschluss der Erbringung der Verarbeitungsleistungen löscht der Auftragsverarbeiter nach Wahl des Verantwortlichen alle personenbezogenen Daten oder gibt sie zurück, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung besteht. Die Löschung wird auf Verlangen in Textform bestätigt.

§ 9 Haftung

Für die Haftung der Parteien gilt Art. 82 DSGVO. Im Übrigen gelten die Haftungsregelungen des EULA.

§ 10 Schlussbestimmungen

(1) Bei Widersprüchen zwischen diesem Vertrag und dem EULA gehen in Fragen der Verarbeitung personenbezogener Daten im Auftrag die Regelungen dieses Vertrags vor.

(2) Änderungen und Ergänzungen dieses Vertrags bedürfen der Textform; dies gilt auch für die Änderung dieses Textformerfordernisses. Die Änderungsmechanik für Unterauftragsverarbeiter nach § 5 bleibt unberührt.

(3) Unterliegt der Verantwortliche dem kirchlichen Datenschutzrecht (KDG oder DSG-EKD), gelten die Verweisungen auf die DSGVO sinngemäß für die entsprechenden Vorschriften des jeweils anwendbaren kirchlichen Datenschutzgesetzes (insbesondere § 29 KDG bzw. § 30 DSG-EKD).

(4) Es gilt das Recht der Bundesrepublik Deutschland. Sollten einzelne Bestimmungen unwirksam sein, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.

Anlage 1 – Gegenstand der Verarbeitung

1. Cloud-Modus (serverseitige Spracherkennung)

Verarbeitung: Entgegennahme von Sprach-/Audiodaten, Umwandlung in Text (Transkription), Rückübermittlung des Textes an das Endgerät des Verantwortlichen. Die Sprach- und Textdaten werden ausschließlich flüchtig zur unmittelbaren Transkription verarbeitet und nicht über den Vorgang hinaus gespeichert.

Datenarten: Sprachaufnahmen und daraus erkannte Texte. Die Inhalte bestimmt allein der Verantwortliche; sie können sämtliche diktierten Angaben enthalten, einschließlich besonderer Kategorien nach Art. 9 DSGVO (z. B. Gesundheitsdaten) sowie Daten Dritter (z. B. Mandanten, Patienten, Geschäftspartner).

Betroffene: Beschäftigte und sonstige Nutzer des Verantwortlichen; Dritte, deren Daten diktiert werden.

2. Support- und Fernwartungsleistungen (optional)

Anlassbezogener Zugriff auf personenbezogene Daten des Verantwortlichen ausschließlich auf dessen Weisung zur Störungsbeseitigung und Unterstützung.

3. Ort der Verarbeitung

Rechenzentrum bzw. Serverinfrastruktur der mit.data GmbH in Deutschland - Emsdetten.

Anlage 2 – Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

Der Auftragsverarbeiter betreibt ein an ISO/IEC 27001 orientiertes Informationssicherheits-Management und trifft insbesondere die folgenden Maßnahmen [vor Einsatz an die tatsächliche Umgebung anpassen]:

1. Vertraulichkeit

- Zutrittskontrolle: gesicherte Serverräume, Zutritt nur für berechtigte Personen, Protokollierung.
- Zugangskontrolle: personalisierte Konten, starke Authentisierung, rollenbasierte Berechtigungen, Sperrkonzept.
- Zugriffskontrolle: Need-to-know-Prinzip, Protokollierung administrativer Zugriffe, regelmäßige Berechtigungsreviews.
- Trennungskontrolle: logische Mandantentrennung der Verarbeitungen je Verantwortlichem.
- Pseudonymisierung: Geräte werden über pseudonyme Kennungen verwaltet; Sprachdaten werden keiner dauerhaften Kennung zugeordnet.

2. Integrität

- Übertragungskontrolle: Transportverschlüsselung (TLS) für sämtliche Verbindungen zwischen Software und Servern.
- Eingabekontrolle: Protokollierung sicherheitsrelevanter Ereignisse und administrativer Änderungen.

3. Verfügbarkeit und Belastbarkeit

- Backup- und Wiederanlaufkonzept für Systeme (nicht für flüchtige Sprachdaten), USV, Monitoring, Patch-Management.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

- Regelmäßige Überprüfung der TOM, Sensibilisierung und Verpflichtung der Beschäftigten, Incident-Response-Prozess, Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen (Art. 25 DSGVO).

Anlage 3 – Unterauftragsverarbeiter

Zum Stand dieses Vertrags setzt der Auftragsverarbeiter **keine Unterauftragsverarbeiter** ein.

Die jeweils aktuelle Liste ist unter www.echologg.com/avv abrufbar. Änderungen erfolgen nach dem Verfahren in § 5 dieses Vertrags (Ankündigung mindestens vier Wochen vorab, Widerspruchsrecht aus wichtigem datenschutzrechtlichem Grund).